We claim:

Sub a1

1. A method of updating keys that decrypt login tickets that log a user into multiple sites, the method comprising:

generating a first key having a first version number;

providing tickets encoded consistent with the first key, the ticket having a version number corresponding to the first version number;

generating a second key having a second version number; and

when the second key becomes current at a site, providing tickets encoded consistent with the second key, the ticket having a version number corresponding to the second version number.

2. The method of claim 1 wherein a different key is provided to each site, and wherein each key is encrypted for decoding at one site.

3. The method of claim 1 and further including generating a configuration file to track keys for each site.

4. The method of claim 1 wherein the key comprises key data and executable code for decrypting tickets.

5. A computer readable medium having instructions stored thereon for causing a computer to perform a method of updating keys that decrypt login tickets that log a user into multiple sites, the method comprising:

generating a first key having a first version number;

providing tickets encoded consistent with the first key, the ticket having a version number corresponding to the first version number;

generating a second key having a second version number; and

when the second key becomes current at a site, providing tickets encoded consistent with the second key, the ticket having a version number corresponding to the second version number.

6. A method of generating keys that decrypt login tickets that log a user into multiple sites, the method comprising:

generating a first key in the form of an executable having a first version number;

generating a second key in the form of an executable having a second version number; and

providing an indication to a login server identifying which key is current for each site such that the tickets are properly encoded.

7. The method of claim 6 and further comprising distributing the key to multiple login servers in a secure manner.

8. The method of claim 6 and further comprising updating a configuration file to track keys for each site.

9. A computer readable medium having instructions stored thereon for causing a computer to perform a method of generating keys that decrypt login tickets that log a user into multiple sites, the method comprising:

generating a first key in the form of an executable having a first version number;

generating a second key in the form of an executable having a second version number; and

providing an indication to a login server identifying which key is current for each site such that the tickets are properly encoded.

10. A system that generates keys that decrypt login tickets that log a user into multiple sites, the system comprising:

a key generator that generates a first key in the form of an executable having a first version number and generates a second key in the form of an executable having a second version number; and

means for providing information to a login server identifying which key is current for each site such that the tickets are properly encoded.

11. A method of updating keys that decrypt login tickets that log a user into multiple sites, the method comprising:

generating a new key with an incremented version number;

sending the new key to a partner site for use in decoding tickets with the incremented version number;

updating key and version information for a login server; and

generating tickets decodable by the new key when an indication that a key having a previous version number has expired.

12. A computer readable medium having instructions stored thereon for causing a computer to perform a method of updating keys that decrypt login tickets that log a user into multiple sites, the method comprising:

generating a new key with an incremented version number;

sending the new key to a partner site for use in decoding tickets with the incremented version number;

updating key and version information for a login server; and

generating tickets decodable by the new key when an indication that a key having a previous version number has expired

13. A method of updating a key used to decrypt tickets used to log into a site, the method comprising:

receiving an updated key with a new version number;

setting a time for an old current key having an old version number to expire;

making the updated key the current key.

14. The method of claim 13 wherein the key comprises executable code for making the updated key the current key.

15. The method of claim 13 and further comprising redirecting users attempting to log into the site using the old current key.

16. A computer readable medium having instructions stored thereon for causing a computer to perform a method of updating a key used to decrypt tickets used to log into a site, the method comprising:

receiving an updated key with a new version number;

setting a time for an old current key having an old version number to expire;

making the updated key the current key.

17. A method of updating a key used to decrypt tickets used to log into a site, the method comprising:

receiving an updated key with a new version number;

setting a time for an old current key having an old version number to expire; and

making the updated key the current key.

18. A computer readable medium having instructions stored thereon for causing a computer to perform a method of updating a key used to decrypt tickets used to log into a site, the method comprising:

receiving an updated key with a new version number;

setting a time for an old current key having an old version number to expire; and

making the updated key the current key.

19. A method of managing keys used to decrypt tickets for logging onto a site, the method comprising:

receiving a first key with a first version number;

encrypting the first key using a hardware address;

changing a current key variable to the first version number;
receiving a new key with an incremented version number;
encrypting the new key using a hardware address; and
identifying the new key as the current key.

20. Them method of claim 19 and further comprising setting a time for the first key identifying when such key may no longer be used.

21. The method of claim 20 wherein a user currently logged in may continue to use the first key until the time expires.

22. The method of claim 20 wherein new user may only use a ticket corresponding to the second key when the second key is made the current key.

23. The method of claim 20 wherein the time is set to a reauthorization time determined by the site.

24. The method of claim 19 wherein a new user using a previous version ticket will be redirected to obtain a ticket corresponding to the new key following the new key being identified as the current key.

25. The method of claim 19 wherein the new key is identified as the current key by changing the current key variable to the second version number.

26. A computer readable medium having instructions stored thereon for causing a computer to perform a method of managing keys used to decrypt tickets for logging onto a site, the method comprising:
receiving a first key with a first version number;
encrypting the first key using a hardware address;
changing a current key variable to the first version number;
receiving a new key with an incremented version number;

encrypting the new key using a hardware address; and

identifying the new key as the current key.

27. A method of updating keys used to decrypt tickets used to log into multiple sites on a network, the method comprising:

generating a new key with a new version number to take the place of an old key with an old version number;

storing the new key on a site to be logged into by a user;

changing a current key indication to the new key;

allowing current logged in users to continue using the old key; and

redirecting new users to a login server to obtain a ticket consistent with the new key.

28. The method of claim 27 wherein the old key may be used by current logged in users for a predetermined amount of time.

29. The method of claim 28 wherein the predetermined amount of time is no more than a reauthorization time by which a current user is normally required to provide login information.

30. The method of claim 28 wherein the predetermined amount of time may be set to zero to force all current and new users to login with a ticket consistent with the new key version.

31. The method of claim 27 wherein the ticket contains a version number consistent with the version number of the key which can decrypt it.

32. The method of claim 27 wherein keys are encrypted by the site using a hardware address, and stored by the site.

33. The method of claim 27 wherein a new key is generated based on a request of the site.

34. The method of claim 27 wherein keys are generated in an executable form which includes key information as well as code for decrypting tickets using the key information.

35. The method of claim 27 wherein the keys are generated by an authentication server, and are distributed to multiple login servers for providing login tickets.

36. A computer readable medium having instructions stored thereon for causing a computer to perform a method of updating keys used to decrypt tickets used to log into multiple sites on a network, the method comprising:

generating a new key with a new version number to take the place of an old key with an old version number;

storing the new key on a site to be logged into by a user;

changing a current key indication to the new key;

allowing current logged in users to continue using the old key; and

redirecting new users to a login server to obtain a ticket consistent with the new key.

37. A method of logging on to multiple sites, the method comprising:

sending a first login ticket to a desired site, wherein the login ticket is encrypted to be decoded by a first key having a first version number;

receiving an indication that the first key has expired;

obtaining a second login ticket from an authentication server, wherein the second login ticket is encrypted consistently with a new key having a second version number; and

sending the second login ticket to the site to log into the site.

38. The method of claim 37 wherein the tickets contain a version number which is readable without decryption.

39. The method of claim 38 wherein the version number is a one digit Hex integer.

40. The method of claim 38 wherein the encrypted ticket comprises an unencrypted version number, and encrypted information sufficient to log a user into a desired site.

41. A computer readable medium having instructions stored thereon for causing a computer to perform a method of logging on to multiple sites, the method comprising:

sending a first login ticket to a desired site, wherein the login ticket is encrypted to be decoded by a first key having a first version number;

receiving an indication that the first key has expired;

obtaining a second login ticket from an authentication server, wherein the second login ticket is encrypted consistently with a new key having a second version number; and

sending the second login ticket to the site to log into the site.

42. An encrypted ticket for use in logging on to a website, the ticket comprising:

an unencrypted version number corresponding to a key version number stored on the website; and

an encrypted string identifying the website and information, which when decrypted using the key having the same version number authenticates the user for logging the user into the website.